REMARKS/ARGUMENTS

Claims 1, 6-10 and 14 remain in this application.

The claims have been amended to be consistent with the specification to obviate the objection.

The Examiner has rejected Claims 1 and 8 under 35 U.S.C. 112, first paragraph. Claims 1 and 8 have been amended. Accordingly, this rejection is obviated.

The Examiner has rejected Claims 1, 5, 7, 10 and 14 as being unpatentable over Richmond in view of Jacobson. Applicant respectfully traverses this rejection.

Referring to Richmond, there is taught controlling concurrent usage of network resources by multiple users at an entry point to a communications network based on identities of the users. Richmond teaches a plurality of users are connected to an entry point of a network by a shared transmission medium. For each of the one or more users, packet rules may be provisioned to the user's entry point to the network where such entry point may be shared with other users. The packet rules may be applied to each packet received from the user for any network resources beyond the entry point are used. These packet rules may be associated with an identity of the user and then provision to the user's entry point in response to the user being authenticated. See paragraphs 109 and 110.

From the above description, and a complete review of Richmond, it is evident that there is no consideration of the possibility of an intruder. Richmond simply discusses whether a user has authorization or not. Richmond does not recognize the situation that intruders can exist who are unauthorized and still obtain access to and consequently compromise networks. Richmond

makes the assumption that if the user does not have any authorization, nothing more will happen. Applicant's claimed invention specifically deals with the situation that there is going to be an intruder, and limits the intruder so the access the traitor has is extremely limited.

Claim 1 has the limitation that the second node cannot use any port between the first and third nodes except for the first and second TCP/IP ports that have been predefined from the first node to the third node and only if the second node is allowed to by the first node, which prevents an intruder who compromises the second network from gaining access to the first network except for the first TCP/IP port. Richmond does not teach or suggest this limitation.

Furthermore, Richmond does not teach or suggest, and is silent in regard to the limitation that the third node only communicating with the first port of the first node through the communication portion via TCP/IP port extension using Gateway methodology which does not connect the first network with the second network.

Referring to Jacobson, there is disclosed a network connection blocker, method, and computer readable memory for monitoring connections in a computer network and blocking the unwanted connections. Jacobson teaches a large computer network with subnets that include host computers. The subnets include a protected a subnet that is protected with a network connection blocker and remote subnets that are remotely connected to the protected subnet. The host computers include local host computers that are within the protected subnet and remote host computers that are within the remote subnets. See column 2, line 66 through column 3, line 7.

The protected subnet includes the network connection blocker that is connected to the protected host computers and the local gateway within the subnet by the communication lines of the subnet. The blocker receives all of the packets transmitted between the protected host computers within the protected subnet at all of the packets transmitted between the protected and

remote host computers. In doing so, the blocker passively monitors all of the connections between the protected host computers and all of the connections between the protected and remote host computers. And, it actively blocks those of the connections that are not wanted by transmitting packets to the host computers that form the unwanted connections to cause these computers to close the unwanted connections. See column 3, lines 41-55.

As is very clear from the above description, Jacobson teaches that the blocker reviews the packets of all connections that exist between any of the host computers and the protected subnet and the host computers in the remote subnets. There is no teaching or suggestion whatsoever of the architecture of applicant's claimed invention. Specifically, there is no teaching or suggestion of a communication portion connecting the first network and the second network only through the first TCP/IP port and a second TCP/IP port that is constant and cannot be changed and which does not connect the first network and the second network. Instead, Jacobson teaches away from this, by providing unlimited connectivity, with the blocker passively reviewing all the connections.

It is respectfully submitted that Jacobson teaches a totally different approach from policing and protecting a network. Furthermore, to the extent that Jacobson may be applicable, it does not prevent an intruder from accessing any aspect of the protected subnet. Jacobson teaches that after the fact, when the connection already exists, it has to be discovered by the blocker so the blocker can then send out packets to cause a computer to close its unwanted connection. Who knows how much damage could have occurred to the protected subnet in that time. Applicant's claimed invention precludes this from even happening. Thus, it is respectfully submitted that the very teaching that the Examiner relies upon from Jacobson to make it obvious to one skilled in the art to have TCP/IP port extension using Gateway methodology, the first TCP/IP port and the second TCP/IP port remain constant and cannot be changed, prevents an intruder who compromises the second network from gaining access to the first network in order

to provide network security by passively monitoring connections between the subnet and the rest of the network and actively blocking those of the connections that are wanted, as the Examiner states on page 5, first full paragraph, teaches away from applicant's claimed invention and does not teach at all with the Examiner purports it to teach.

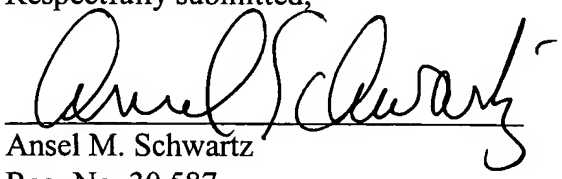
Accordingly, Claim 1 is patentable over Richmond and Jacobson. Claims 6 and 7 are dependent to parent Claim 1 and are patentable for the reasons Claim 1 is patentable. Claim 10 is patentable for the reasons Claim 1 is patentable. Claim 14 is dependent to Claim 10 and is patentable for the reasons Claim 10 is patentable.

The Examiner has rejected Claims 8 and 9 as being and patentable over Richmond in view of Jacobson and Border. Applicant respectfully traverses this rejection in view of the amendments to the claims.

Referring to Border, there is taught a method and system for communicating over a segmented virtual private network. Border teaches to use an encrypted tunnel to control access between private networks. Like Richmond, Border does not actually deal with the situation of an intruder that does gain access to a network and how to limit the effects of the intruder. It is respectfully submitted that Border adds nothing to the teachings of Richmond to arrive at applicant's claimed invention, as amended. Claims 8 and 9 are dependent to parent Claim 1 and are patentable for the reasons Claim 1 is patentable over the applied art of record.

In view of the foregoing amendments and remarks, it is respectfully requested that the outstanding rejections and objections to this application be reconsidered and withdrawn, and Claims 1, 6-10 and 14, now in this application be allowed.

Respectfully submitted,



Ansel M. Schwartz
Reg. No. 30,587
201 N. Craig Street, Suite 304
Pittsburgh, PA 15213
Tel.: (412) 621-9222